Claims

1. A method for retrieving digital objects from a group of digital objects maintained by a database, the group of digital objects being represented by the equation $G = \{m_i, i = 1, 2, ..., N\}$, wherein G represents the group of digital objects, N represents the number of digital objects maintained by the database, i represents an index having allowable values between 1 and N inclusive, and m_i represents an ith digital object within the group of digital objects, the method comprising:

generating a random number R and keys k_i, i having allowable values between 1 and N inclusive, for a symmetric key cryptosystem;

determining a prime number p;

encrypting digital object m_i with key k_i using the symmetric key cryptosystem to obtain ciphertext c_i;

assigning a value of k_i^R mod p to a key ciphertext $s_{i;}$

responsive to the database receiving a request signal from a user, sending c_i, and s_i to the user;

receiving from the user a number n of input signals W_j, such that n is less than N, and j is an index having allowable values between 1 and n inclusive;

computing changed ciphertext U_j, such that U_j is equal to $W_j^{1/R \bmod (p-1)}$ mod p; and

sending U_j to the user.

2. The method of claim 1, where the modulo operations may be carried out in any group in which a discrete logarithm is infeasible to compute.

3. A method for a user to privately retrieve digital objects from a group of digital objects G = { m_i, i = 1, 2, ..., N) maintained by a database, the method comprising the steps of:

sending a request signal to the database;

receiving reply signals c_i, s_i, l = 1, 2, ..., N from the database;

generating random numbers w_j, computing and sending $W_j = s_{ij}^{wj}$ mod p, j = 1, 2, ..., n to the database;

receiving signals U_j, j = 1, 2, ..., n from the database;

computing $k_{ij} = Uj^{1/wj \bmod (p-1)}$ mod p, j = 1, 2, ..., n; and

decrypting c_{ij} with k_{ij} and a symmetric key cryptosystem to recover digital objects m_{ij}, j = 1, 2, ..., n.

4. The method of claim 3, wherein the modulo operations may be carried out in any group in which a discrete logarithm is infeasible to compute.

5. A method for selectively retrieving digital objects from a database of digital objects using a symmetric key cryptosystem, the method comprising:

for each digital object in the database:

generating a unique key for the symmetric key cryptosystem;

associating the key with the digital object;

encrypting the digital object using the associated key and the symmetric key cryptosystem to produce a ciphertext of the digital object;

encrypting the associated key to obtain a ciphertext of the key;

transmitting the ciphertext of the digital object and the ciphertext of the key associated with the digital object to a user;

receiving at least one changed ciphertext of the keys associated with the digital objects in the database;

decrypting each received changed ciphertext; and

transmitting the decrypted received changed ciphertexts.

6. A method for retrieving digital objects from a group of digital objects maintained by a database, the method comprising the steps of:

selectively requesting a plurality of digital objects from the database;

receiving encrypted ciphertext digital objects from the database;

receiving from the database encrypted ciphertext keys associated with the received ciphertext digital objects;

encrypting at least one of the encrypted ciphertext keys to obtain changed ciphertext keys;

sending the changed ciphertext keys to the database;

receiving partially decrypted changed ciphertext keys from the database;

decrypting the partially decrypted changed ciphertext keys; and

decrypting at least one of the received ciphertext digital objects using the decrypted keys.

7. An apparatus comprising:

a computerized database;

coupled to the database, a computer user;

coupled to the database, a transmitting module for transmitting data to the user;

coupled to the database, a receiving module for receiving data from the user;

coupled to the database, a random number generating module for generating random numbers;

coupled to the database, a key generating module for generating cryptographic keys;

coupled to the database, an encrypting module for encrypting data;

coupled to the database, a decrypting module for decrypting data;

coupled to the user, a requesting module for requesting data from the database;

coupled to the user, a transmitting module, for transmitting data to the database;

coupled to the user, a receiving module, for receiving data from the database;

coupled to the user, a random number generating module for generating random numbers;

coupled to the user, an encrypting module for encrypting data; and

coupled to the user, a decrypting module for decrypting data.

8. A computer program product stored on a computer readable medium for retrieving digital objects from a group of digital objects maintained by a database, the computer program product controlling a processor coupled to the medium to perform the operations of:

for each digital object in the database:

generating a unique key for a symmetric key cryptosystem;

associating the key with the digital object;

encrypting the digital object using the associated key and the symmetric key cryptosystem to produce a ciphertext of the digital object;

encrypting the associated key to obtain a ciphertext of the key;

transmitting the ciphertext of the digital object and the ciphertext of the key associated with the digital object to a user;

receiving at least one changed ciphertext of the keys associated with the digital objects in the database;

decrypting each received changed ciphertext; and

transmitting the decrypted received changed ciphertexts.